Christopher J. Schatz, OSB No. 915097
Assistant Federal Public Defender
101 SW Main Street, Suite 1700
Portland, OR 97204
Tel: (503) 326-2123
Fax: (503) 326-5524
Email: chris_schatz@fd.org

Attorney for Hock Chee Khoo

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,	**CR 09-321-KI**
Plaintiff,	**DECLARATION OF COMPUTER FORENSICS EXPERT MICHAEL A. BEAN IN SUPPORT OF MOTION TO EXCLUDE IMAGES OF THE WU LAPTOP HARD-DRIVE.**
vs.	
HOCK CHEE KHOO, et al.,	
Defendants.	

I, Michael Bean, declare:

1. I am an expert in computer forensics, and I have been recognized as such. I have testified as a computer forensics expert in both federal and state court. I previously served in law enforcement as the lead detective of a computer crime squad for the Gwinnett County police department located in Lawrenceville, Georgia, for 3 years. Subsequent to that assignment I served as a Master Instructor and Senior Manager for Guidance Software, the creator of the EnCase

computer forensic software, where I instructed over 300 students in the use of EnCase as an investigative platform in the practice of computer forensics from the beginner to advanced levels. I have received training in and I have used a variety of computer forensic software programs, including Forensic Tool Kit (FTK), EnCase, and others in the course of conducting forensic examinations of computer hard-drive data contents and configurations. I have been awarded EnCase certification by virtue of successfully passing both the written and practical components of the EnCE testing program. I am currently the President of In2itive Technologies, a company specializing in the processing of data for electronic discovery used in litigation and computer forensic examination and analysis. True and accurate copies of my current Curriculum Vitae and EnCase certification are attached hereto as Exhibit A.

2. I was previously engaged on March 24, 2010, by the Federal Public Defender's Office for the District of Oregon to provide ongoing expert computer forensic analysis and assistance to Assistant Federal Public Defender Christopher J. Schatz, attorney for Hock Chee Khoo, in the above-entitled case.

3. At the request of AFPD Schatz, I have examined two digital images associated with this case that are alleged to be images of the hard drive data configuration of a laptop computer ("Laptop image") and an external hard drive ("Acronis image") containing a subset of the data on the laptop. It is my understanding, based on information provided to me by AFPD Schatz, that the afore-referenced digital images are images taken of the hard drive of a laptop computer, belonging to The Hoffmann Group (THG), that was previously in the sole custody of an individual known as Shengbao (Jesse) Wu. It is my further understanding that, on October 17, 2006, the afore-referenced laptop computer (also referred hereinafter to as the "Wu Laptop") was taken from Wu's custody by

Drew Hoffman and Mark Hansen. It is my further understanding that Hansen moved a folder named "Private" from a location on the Wu Laptop file system to the desktop area of the file system recognized by the computer, and that thereafter Hansen copied (*i.e.* created a backup file of) the Private folder and files within the folder to an external hard drive using Acronis software. I am further informed that between October 17 and October 20, the Wu Laptop was in the custody of Drew Hoffman and that certain additional modifications to the data configuration on the Wu Laptop were made by Hoffman. I am further informed that, on October 20, 2006, the Wu Laptop and the exterior hard drive containing the Acronis image were transported to FBI's Northwest Regional Computer Forensics Laboratory (NWRCFL), where the digital images I have examined were made by FBI Special Agent Joel Brillhart. These digital images consist of (1) an FBI image of the external hard drive containing the backup file allegedly created by Mark Hansen on October 17, 2006, using Acronis software (the "Acronis image"); and (2) a digital image allegedly of the Wu Laptop (the "Laptop image") created by SA Brillhart using Forensic Tool Kit software.

4. After reviewing both the Acronis image and the Laptop image, I have come to several conclusions based on my expertise in the field of computer forensics. These conclusions, reflected in the findings hereinafter discussed, raise significant questions concerning the reliability of the processes used to create the Acronis and Laptop images and the ability to determine to an adequate degree of forensic confidence whether (or to what extent) either image accurately reflects the data contents and configuration of the Wu Laptop hard drive prior to its being seized by Hoffman and examined by Hansen on October 17, 2006.

5. The Acronis software used by Hansen to create the backup file of the Private folder is not a software tool that is appropriate for producing reliable and accurate forensic images that satisfy forensic examination standards. Acronis was designed as an archival tool that, once installed on a target computer, allows a user to selectively choose data from that computer to copy on a file-by-file basis. This is called accessing data at the "logical" level,[1] and means that one must be using the target computer to extract data contained therein. Reliable forensic standards require use of software specifically designed for computer forensic purposes which will copy a computer at what is known as a "physical" level,[2] producing a bit-for-bit copy known as a "forensic image." This forensic software is not installed on the target computer, but on a secondary computer which will then be used to access the target in a fashion that protects the target from changes. When the target is then accessed, a bit-for-bit copy, or "forensic image" of the target is made which preserves potentially volatile information that is, or can be, lost when a user logs in to the target machine.

6. Hansen's installation of Acronis software on the Wu Laptop contravened standard forensic procedures. By installing the Acronis software, Hansen altered the contents and data configuration of Wu's hard drive. Such alteration follows as a matter of course given that new information often occupies hard-drive space previously allocated to "deleted" information. By

[1] Capturing a file at a logical level will only capture the content of the file based on the file size in bytes and does not capture the remaining unused defined area of the cluster that the file is occupying. As an example, if a disc has a sector size of 512 bytes arranged in clusters of 2 (2 sectors per cluster) that would yield an allocated area of 1024 bytes. If a file in that allocated cluster was only 600 bytes, there would be an additional 424 bytes of data that would not be collected.

[2] Using the example in footnote 1, accessing a file at the physical level will capture all 1024 bytes, *i.e.* the content of the logical file and the remaining data in the cluster from the end of the logical file to the end of the assigned cluster.

supplanting "deleted" information, the new information (in this instance, the compressed Acronis software download package, the extraction and installation of the uncompressed program and additional files created via the usage of the Acronis software) renders the deleted information in the previously allocated drive space permanently inaccessible.

7. The Laptop image data confirms that Hansen moved the contents of a folder named "Private" from the Wu Laptop "C" drive to the desktop prior to producing the Acronis backup file. Hansen's activity in this regard would have displaced a significant amount of previously deleted data. Given the size of the resulting file, it is likely that a significant amount of otherwise recoverable information has been permanently displaced, including the directory structure as it existed prior to the folder's being moved.

8. Examination of the date and time information pertaining to the Laptop image indicates that, after moving the "Private" folder and its contents to the desktop, over an hour elapsed before Hansen actually attempted to create the Acronis backup file. It cannot be determined what occurred during that time period, with respect to the data content and configuration on the Wu Laptop, because the resulting Acronis backup file only contains selected contents of the "Private" folder.

9. The Laptop image also contained log files that were created by the Acronis software. These logs indicate that Hansen made three attempts to create the Acronis backup file, with only the final attempt being successful. I can attest that the process of creating digital images where a write blocking device is not employed causes damage to information stored on a hard drive – damage which can be exacerbated by multiple attempts.

10. On the basis of a report purportedly created by Hansen, and the dates associated with the creation of the Acronis backup file, I have determined that the active Acronis backup file that Hansen made was produced no later than 01:40:44 a.m. on October 18, 2006 (China time). A copy of the Hansen report and an FBI 302 interview report regarding Hansen are attached hereto as Exhibit B.

11. Examination of the data from the Laptop image indicates that, while the Laptop was in Hoffman's possession, he created a desktop folder on the computer entitled "QQ." The creation of this file would have effected the Wu Laptop, in the same way as the installation of the Acronis software and the creation of the "Private" desktop folder, by displacing information stored in the hard-drive's allocated space.

12. The Acronis image (the image of the device containing the backup file created by Hansen on October 17) is dated October 3, 2006. I am unable to come to a conclusion based on information currently available to me as to why there is a forensic image in existence with a creation date prior to the dates of the files contained on the Wu Laptop hard drive that was forensically imaged.

13. Analysis of the contents of the Laptop image reveals that there are over 1000 files or folders with dates of creation after 01:40:44 a.m. on October 18, 2006 (China time). The latest date of creation is October 21, 2006. Based on my examination of the Laptop image, I have come to the conclusion that there are over 1000 files or folders that were accessed, manipulated, or created after

the date of creation associated with Hansen's Acronis backup file.[3] In addition, several executable files were installed on the Wu Laptop computer.[4]

14. Similar to the Acronis image, the Laptop image has a creation date predating the date of creation associated with files in the Hansen Acronis backup file. The date of creation associated with the Laptop image is October 5, 2006. Again, I am unable to come to a conclusion based on information currently available to me as to why there is a forensic image in existence with a creation date that is prior to the dates of the files contained on the hard-drive that was forensically imaged.

15. In contrast to the procedures used by the FBI to produce the Acronis and Laptop images, in my opinion, a proper forensic imaging protocol of the Wu Laptop computer would have involved the following steps:

(a) The devices (the Wu Laptop and the removable exterior hard drive device used by Hansen) would have been provided to a properly trained and currently certified FBI forensic computer examiner;

(b) The FBI examiner would have documented the make, model, and serial number of the hardware containing the data to be imaged;

[3] Given the lack of forensic supporting and confirming documentation pertaining to the examination tools and procedure utilized by SA Brillhart, and the current data content and configuration of the Laptop and Acronis images, it is not forensically possible, to any acceptable degree of confidence, to distinguish between files that were merely accessed, files that were modified or changed, and files that were created on the Wu Laptop following creation of the Acronis backup file.

[4] An "executable file" is a file that causes a computer to perform indicated tasks according to encoded instructions, as opposed to a data file that must be parsed by a program to be meaningful.

(c) The FBI examiner would have obtained any CMOS or BIOS setting for any device that had a CPU;[5]

(d) The hard drives would have been removed from the Wu Laptop and the removable exterior device provided by Hansen;

(e) The FBI examiner would have documented the make, model, serial number and size of the hard-drives;

(f) The FBI examiner would have connected the hard drives to hardware write-blockers so that no changes could be made to the hard drives during the imaging process;

(g) The FBI examiner would have then documented the type of hardware write blocker used and any malfunction if any observed;

(h) The FBI examiner would have created forensic images of the hard drives; and

(i) The FBI examiner would have documented all relevant identification information with respect to the software and hardware used to create the forensic images.

16. In producing the Acronis and Laptop images , SA Brillhart materially deviated from standard forensic procedures. Specifically, SA Brillhart's examination and image capture procedure was deficient in the following ways:

(a) There is no documentation (to my knowledge) concerning the forensic imaging hardware, software or procedure utilized;

[5] CMOS is short for "complementary metal oxide semiconductor." Personal computers contain a small amount of battery-powered CMOS memory to hold the date, time, and system setup parameters. BIOS is an acronym for basic input/output system, the built-in software that determines what a computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions.

(b) There is no documentation (to my knowledge) concerning the devices that were imaged (*i.e.*, pictures, logs, worksheets, etc.);

(c) There is no documentation (to my knowledge) of any CMOS or BIOS data from the devices that should have been documented at the time of the imaging;

(d) There is no documentation (to my knowledge) as to identifying information concerning the imaged hard drives, including, but not limited to, make, model, serial number, size, jumper settings, etc.;

(e) There is no documentation (to my knowledge) as to what equipment the FBI used to make the Laptop and Acronis images (hardware and software); and

(f) The computer equipment used to make the Laptop and Acronis images does not appear to have been properly time and date calibrated.

17. Based on the foregoing findings and conclusions, it is my expert opinion that no forensic expert, let alone any lay person, could conclude with any degree of certainty that the information on the Acronis and Laptop images accurately reflects the data contents and configuration of the Wu Laptop computer as such existed prior to the time it was seized by Hoffman and Hansen on October 17, 2006.

I declare under perjury under the laws of the United States of America that the foregoing statements are true and correct to the best of my knowledge and belief, and that this Declaration was executed on May 27th, 2010, in Portland, Oregon.

Michael Bean